

**GOVERNMENT OF INDIA
HOME AFFAIRS
LOK SABHA**

UNSTARRED QUESTION NO:452

ANSWERED ON:01.12.2015

Online Fraud

Ram Shri Vishnu Dayal

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) the number of cases registered regarding online fraud during each of the last three years and the current year, State-wise;
- (b) the action taken by the Government and the number of cases disposed of in this regard during the said period, State-wise;
- (c) whether the Government is aware that online fraud is being done by the Nigerians on a very large scale in the country; and
- (d) if so, the efforts being made by the Government to stop such cases in future?

Answer

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI HARIBHAI PARATHIBHAI CHAUDHARY)

(a) : The State/UT wise number of cases reported regarding forgery (under sections Indian Penal Code of 405, 468 & 471) using computer as medium/target under cyber crime during 2012- 2014 is enclosed at Annexure-I. National Crime Records Bureau (NCRB) has also started collecting data on cheating using computer as medium/target under cyber crime since 2014. State/UT wise cases reported under cheating (sec. 420 IPC) during 2014 is enclosed Annexure-II.

(b): NCRB has started collecting data on cases disposed of under such crimes since 2014. State/UT wise cases reported, cases charge-sheeted and cases convicted under forgery & cheating using computer as medium/target under cyber crime is enclosed at Annexure-III.

...2/-

-2-

LS.U.Q.No. 452 for 01.12.2015

(c): The Government is aware of the media reports regarding some online fraud being done by Nigerians. Specific information in this regard is not maintained centrally.

(d): The major remedial measures taken by the Government in this regard are as under:-

(i) Indian Computer Emergency Response Team (CERT-In) is working in coordination with Reserve Bank of India (RBI) and banks to track and disable phishing websites.

(ii) Banks have implemented Two-factor authentication to mitigate risks due to theft of online credentials. Besides, SMS alerts are sent to users intimating details of transactions involving amounts above specified threshold.

(iii) To create awareness about possible frauds by using email and SMS, advisories are being issued by Banks, Telecom Service Providers and Police Authorities from time to time to the users.

(iv) Banks are creating user awareness for general public against phishing, lottery scams, internet banking, Credit/Debit cards and other frauds. Steps have been taken to monitor and prevent financial frauds through phishing attacks, Credit / Debit card frauds, money laundering schemes etc.

(v) Indian Computer Emergency Response Team (CERT-In) has published whitepaper on countering phishing attacks and regularly conducts training programme for system administrators and general users in the Government, public and private sector on countering cyber frauds and phishing attacks.

(vi) The Information Technology Act, 2000, provides legal framework to address various types of prevalent cyber crimes and security breaches of information technology infrastructure.

(vii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

...3/-

-3-

LS.U.Q.No. 452 for 01.12.2015

(viii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

- (ix) Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
- (x) Number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed and are being used by Law Enforcement Agencies.
- (xi) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
- (xii) Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.
- (xiv) Department of Electronics & Information Technology (DeiTY) is conducting programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security.
